CLAIMS

What is claimed is:

1. A method of reducing computation during each Data Encryption Standard (DES) encryption and decryption round, the method comprising the steps of:

a) generating at least one large SP-box lookup table;

b) computing an index for each SP-box lookup table;

c) adding operations to the DES round key computation function to obtain a modified round key computation function; and

d) computing the index for each SP-box by performing XOR operations between at least one block of contiguous bits of the input to the DES Expansion Permutation and said modified round key computation function.

2. A method of reducing the number of software instructions required to perform permutation and substitution operations using Data Encryption Standard (DES) encryption and decryption rounds, wherein each round has a 64-bit input, and 32 bits of that 64-bit input are applied as the input to the DES Expansion Permutation, the method comprising the steps of:

a) generating at least one large SP-box lookup table;

b) adding operations to the DES round key computation function to obtain a modified round key computation function;

c) computing a modified SP-box index by performing XOR operations between at least one block of contiguous bits of the 32-bit input to the DES Expansion Permutation and the result of the modified round key computation function of step b); and

d) executing each subsequent round of DES computation by repeating steps a) and c).

3. The method recited in claim 2, wherein steps a) through d) are carried out in a digital processor.

4. The method recited in claim 3, wherein said digital processor is taken from the group consisting of a general-purpose processor, an embedded processor and a cryptographic processor.

5. The method recited in claim 2, wherein step c) comprises the step of selecting two blocks of contiguous bits of the 32-bit input to DES Expansion Permutation.

6. The method recited in claim 5, wherein one of said two blocks includes the least significant bit of said 32-bit input and the other of said two blocks includes the most significant bit of said 32-bit input for each of said round.

7. The method recited in claim 2, wherein step c) is carried out by permuting the entries within each SP-box lookup table.

8. In a processor carrying out a Data Encryption Standard (DES) computation by iterative DES rounds, a method of reducing computation associated with the DES Expansion Permutation by reducing the number of instructions required to compute the inputs to DES SP-boxes, the method comprising the steps of:

a) mathematically transforming the DES round function in each said round;

b) mathematically transforming the DES round key computation function in each said round; and

c) modifying the inputs to said SP-boxes in accordance with the results of steps a) and b).

9. The method recited in claim 8, wherein steps a) and b) are carried out so that computation in the DES Expansion Permutation is shifted from the DES round function to the DES round key computation function.

10. An apparatus for reducing computation during each Data Encryption Standard (DES) encryption and decryption round, the apparatus comprising:

a) means for generating at least one large SP-box lookup table;

b) means for computing an index for each SP-box lookup table;

c) means for adding operations to the DES round key computation function to obtain a modified round key computation function; and

d) means for computing the index for each said SP-box by performing XOR operations between at least one block of contiguous bits of the input to the DES Expansion Permutation and said modified round key computation function.

11. An apparatus for reducing the number of software instructions required to perform permutation and substitution operations in the Data Encryption Standard (DES) encryption and decryption rounds, wherein each round has a 64-bit input and 32 bits of that 64-bit input are applied as the input to the DES Expansion Permutation, the apparatus

comprising:

a) means for generating at least one large SP-box lookup table;

b) means for adding operations to the DES round key computation function to obtain a modified round key computation function; and

c) means for computing a modified SP-box index by performing XOR operations between at least one selected block of said 32-bit input to the DES Expansion Permutation and the result of the modified round key computation function.

12. The apparatus recited in claim 11, wherein said means for computing comprises a digital processor.

13. The apparatus recited in claim 12, wherein said digital processor is taken from the group consisting of a general-purpose processor, an embedded processor and a cryptographic processor.

14. The apparatus recited in claim 11, wherein said means for computing comprises means for selecting two blocks of said 32-bit input to the DES Expansion Permutation.

15. The apparatus recited in claim 14, wherein one of said two blocks includes the least significant bit of said 32-bit input and the other of said two blocks includes the most significant bit of said 32-bit input for each of said round.

16. The apparatus recited in claim 11, wherein said means for generating

comprises means for permuting the entries within each said SP-box lookup table.

17. In a processor carrying out a Data Encryption Standard (DES) computation by iterative DES rounds, an apparatus for reducing computation associated with the DES Expansion Permutation by reducing the number of instructions required to compute the inputs to DES SP-boxes, the apparatus comprising:

a) means for mathematically transforming the DES round function in each said round;

b) means for mathematically transforming the DES round key computation function in each said round; and

c) means for modifying the inputs to said SP-boxes in accordance with the transformations of said round function and of said round key computation function.

18. The apparatus recited in claim 17, wherein means for modifying comprises means for shifting computation in the DES Expansion Permutation from the DES round function to the DES round key computation function.

19. A data processing system for carrying out Data Encryption Standard (DES) encryption and decryption rounds with reduced computation, the system comprising:

a) computer processing means for processing data;

b) storage means providing four large SP-box lookup tables;

c) means for computing indices for the respective SP-box lookup tables;

d) means for adding operations to the DES round key computation function to obtain a modified round key computation function; and

e) means for computing the index of each said SP-box by performing XOR operations between at least one block of contiguous bits of the input to the DES Expansion Permutation and said modified round key computation function.